

REMARKS

Claims 1, 3-26 are pending. No claim amendments are made with this response. Reconsideration of the application is respectfully requested based on the following remarks.

I. REJECTION OF CLAIMS 1, 3, 4, 6, 9-21, 23, 26-32 and 34 UNDER 35 U.S.C. § 103(a)

Claims 1, 3, 4, 6, 9-21, 23, 26-32 and 34 were rejected under 35 U.S.C. § 103(a), as being unpatentable over U.S. Patent No. 7,142,671 (Qi et al.) in view of Anand U.S. Patent No. 7,280,657. Withdrawal of the rejection is respectfully requested for at least the following reasons.

- i. Neither Qi et al. nor Anand teach the cipher output of the eight cipher blocks feedback coupled to the second input of the data input multiplexer and to the first input of a pre-data output multiplexer, as recited in claims 1 and 19.*

The Office Action dated 07/18/08, in the “Response to Arguments” section page 15 (last line) through page 16, first paragraph, points out (See, *e.g.*, MPEP § 707.07(f), paragraph 7.37.09) that “A recitation of the intended use of the claimed invention must result in **structural difference** between the claimed invention and the prior art in order to **patentably distinguish** the claimed invention from the prior art.” The applicant agrees with the examiner in this regard, and further with the Office Action which concedes on page 16 that “**the prior art Qi and Anand have different structures from the claimed invention but they perform a similar function and provide similar results as claimed**”. Here again, the applicant agrees that the **claimed invention has, in fact, numerous structural differences** (*e.g.*, as (*i*) indicates above) **between the claimed invention and the prior art**. Therefore, the claimed invention has been **patentably distinguished from the prior art**, for example, as is explained further below.

Claims 1 and 19 are directed to a security processing circuit that comprises a DES engine. The DES engine further comprises eight cipher blocks operable to output first and second results of a sequential eight step cipher process during a first and second eight step cycle of each of the three DES processing operations. The final “wherein clause” of claims 1 and 19 further define a unique structural configuration, reciting that *the cipher output of the eight cipher blocks is **feedback coupled to the second input of the data input multiplexer and to the first input of a pre-data output multiplexer*** to facilitate the 3DES processing. Neither Qi et al. nor Anand teach this structural feature.

By contrast, Qi et al. teach, a feedback timing critical path 451 of Fig. 4B, which is structurally configured to feed only right side cipher data back to an input mux 409 without any such additional structural interconnection directly to a pre-data output mux, as shown in Figs. 4A and 4B. Rather, feedback path 451 only connects a Right last round register 435 to an input mux 409, **but neither Qi et al. nor Anand connect to a pre-data output multiplexer to receive the cipher results as recited in claims 1 and 19.** In addition, the output of the **SBOX 427 of Qi** (which page 15 of the Office Action appears to compare to the 8 cipher blocks 81d of the claimed invention), **connects only to a permutation stage 429**, which thereafter connects to a summing element 431 (that adds the left-side cipher data) **before the feedback path 451.** Therefore neither Qi et al. nor Anand teach the structure of the invention of claims 1 and 19.

In addition to the structural differences highlighted above, claims 1 and 19 further provide other structurally distinguishing elements, for example:

- 1) *wherein **the latched data output of the intermediate result register is coupled to the data input of the eight cipher blocks,***
- 2) ***the data selection output of the pre-data output multiplexer coupled to the pre-data output register,***

- 3) ***the latched data output of the pre-data output register feedback coupled to the second input of the pre-data output multiplexer and the pre-data output.***

In one non-limiting example of Fig. 1J of the present invention, ***the latched data output of the intermediate result register (81c) is coupled to the data input of the eight cipher blocks (81d), the data selection output of the pre-data output multiplexer (81e) coupled to the pre-data output register (81f), the latched data output of the pre-data output register (81f) feedback coupled to the second input of the pre-data output multiplexer (81e) and the pre-data output (e.g., feedback connection between 81f and 81e).*** Neither Qi et al. nor Anand teach these additional structurally distinguishing features of the invention of claims 1 and 19.

Accordingly, withdrawal of the rejection is respectfully requested.

II. REJECTION OF CLAIMS 5, 7, 8, 22, 24 and 25 UNDER 35 U.S.C. § 103(a)

Claims 5, 7, 8, 22, 24 and 25 were rejected under 35 U.S.C. § 103(a), as being unpatentable over U.S. Patent No. 7,142,671 (Qi et al.) in view of Anand (U.S. Patent No. 7,280,657) and in view of Callum (US Patent No. 6, 985,581). Withdrawal of the rejection is respectfully requested for at least the following reasons.

As indicated above, Claims 1 and 19 are neither taught by Qi et al. nor Anand. Claims 5, 7 and 8 depend from independent claim 1 and claims 22, 24 and 25 depend from claim 19, which are believed to be allowable over Qi et al. and Anand for, at least, the foregoing reasons. The addition of Callum fails to make up for the aforementioned deficiencies of Qi et al. and Anand with regard to independent claim 1, and thus claims 5, 7 and 8 are believed to be allowable over the suggested combination. Claims 22, 24 and 25 are thus also believed to be allowable over the suggested combination as they depend from independent claim 19.

Accordingly, withdrawal of the rejection is respectfully requested.

III. TERMINAL DISCLAIMER FILING

Applicant acknowledges with appreciation the filing of the terminal disclaimer on May 2, 2008 and the corresponding withdrawal of the provisional double patenting rejection.

IV. CONCLUSION

For at least the above reasons, the claims currently under consideration are believed to be in condition for allowance.

Should the Examiner feel that a telephone interview would be helpful to facilitate favorable prosecution of the above-identified application, the Examiner is invited to contact the undersigned at the telephone number provided below.

Should any fees be due as a result of the filing of this response, the Commissioner is hereby authorized to charge the Deposit Account Number 50-1733, AMDP782US.

Respectfully submitted,
ESCHWEILER & ASSOCIATES, LLC

By /Thomas G. Eschweiler/
Thomas G. Eschweiler
Reg. No. 36,981

National City Bank Building
629 Euclid Avenue, Suite 1000
Cleveland, Ohio 44114
(216) 502-0600